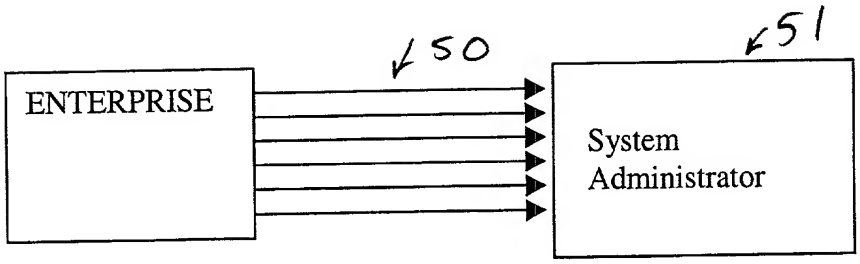


PRIOR ART

Figure 1

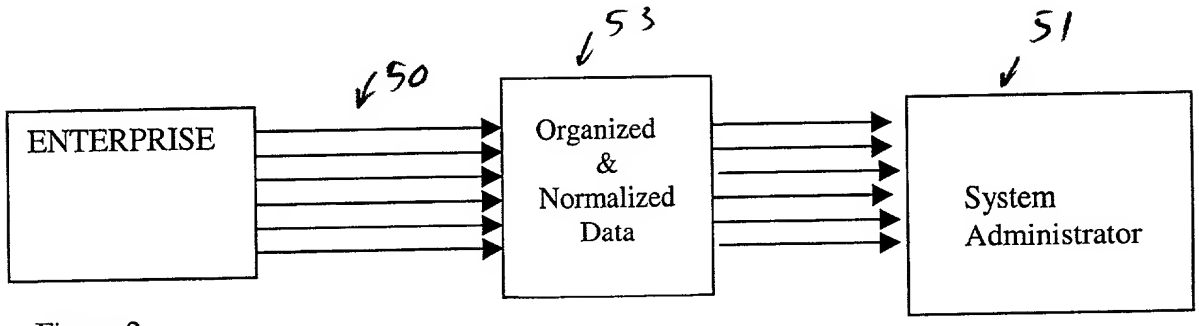
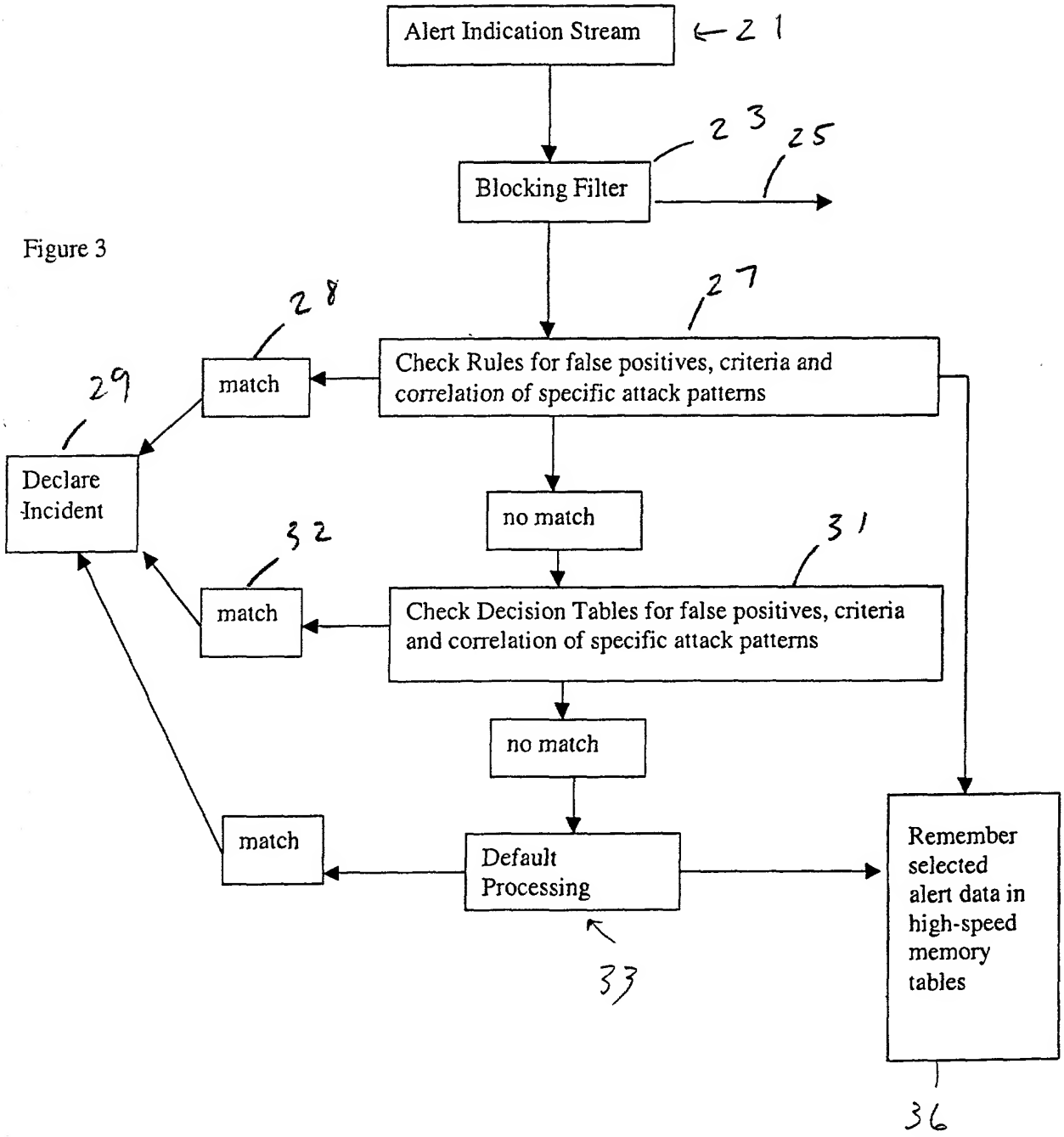


Figure 2

PRIOR ART

Figure 3


Alert Indication Stream
21
23
25
Blocking Filter
27
28
match
Check Rules for false positives, criteria and correlation of specific attack patterns
29
Declare Incident
no match
31
32
match
Check Decision Tables for false positives, criteria and correlation of specific attack patterns
no match
match
Default Processing
33
Remember selected alert data in high-speed memory tables
36

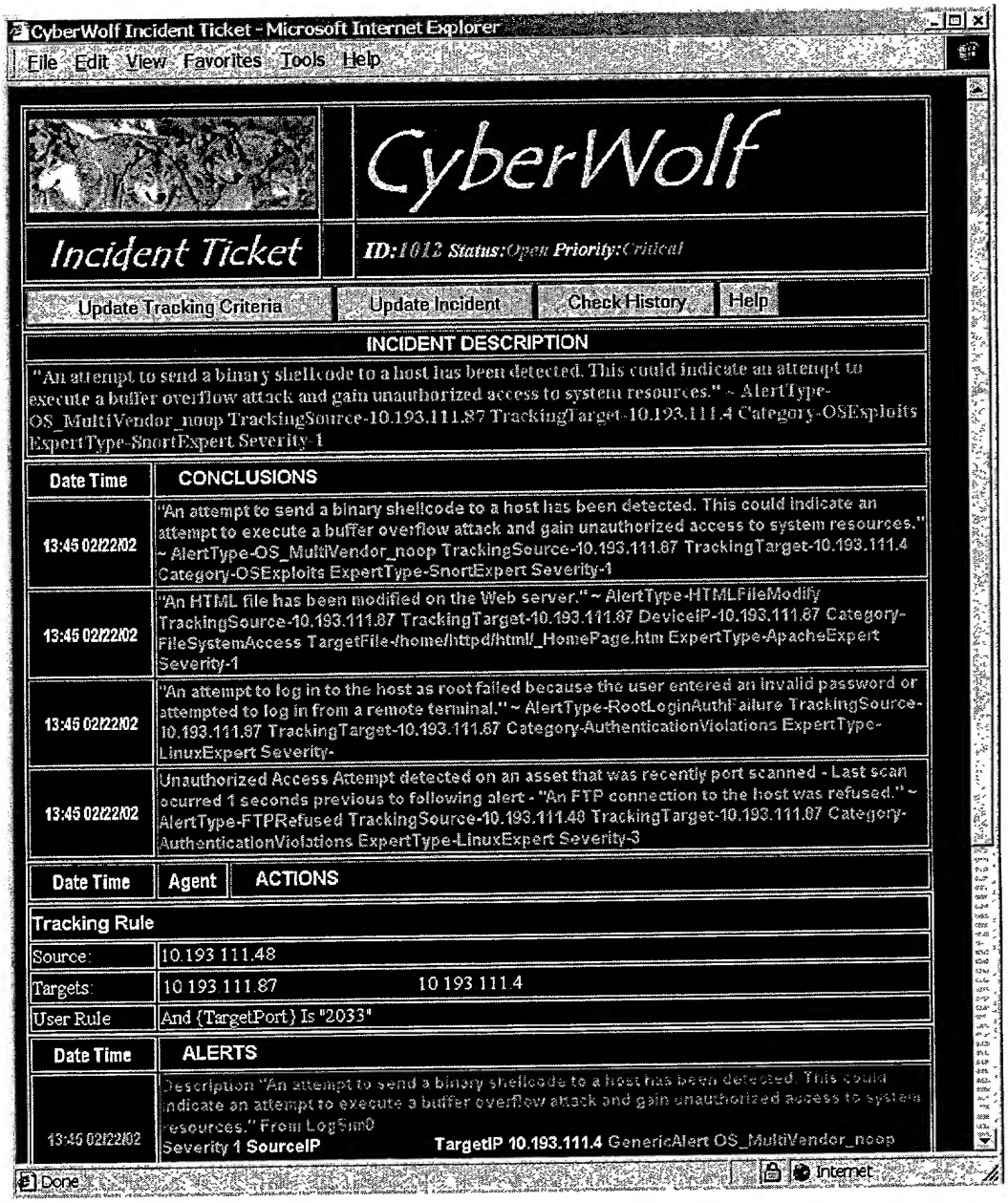


Fig. 4

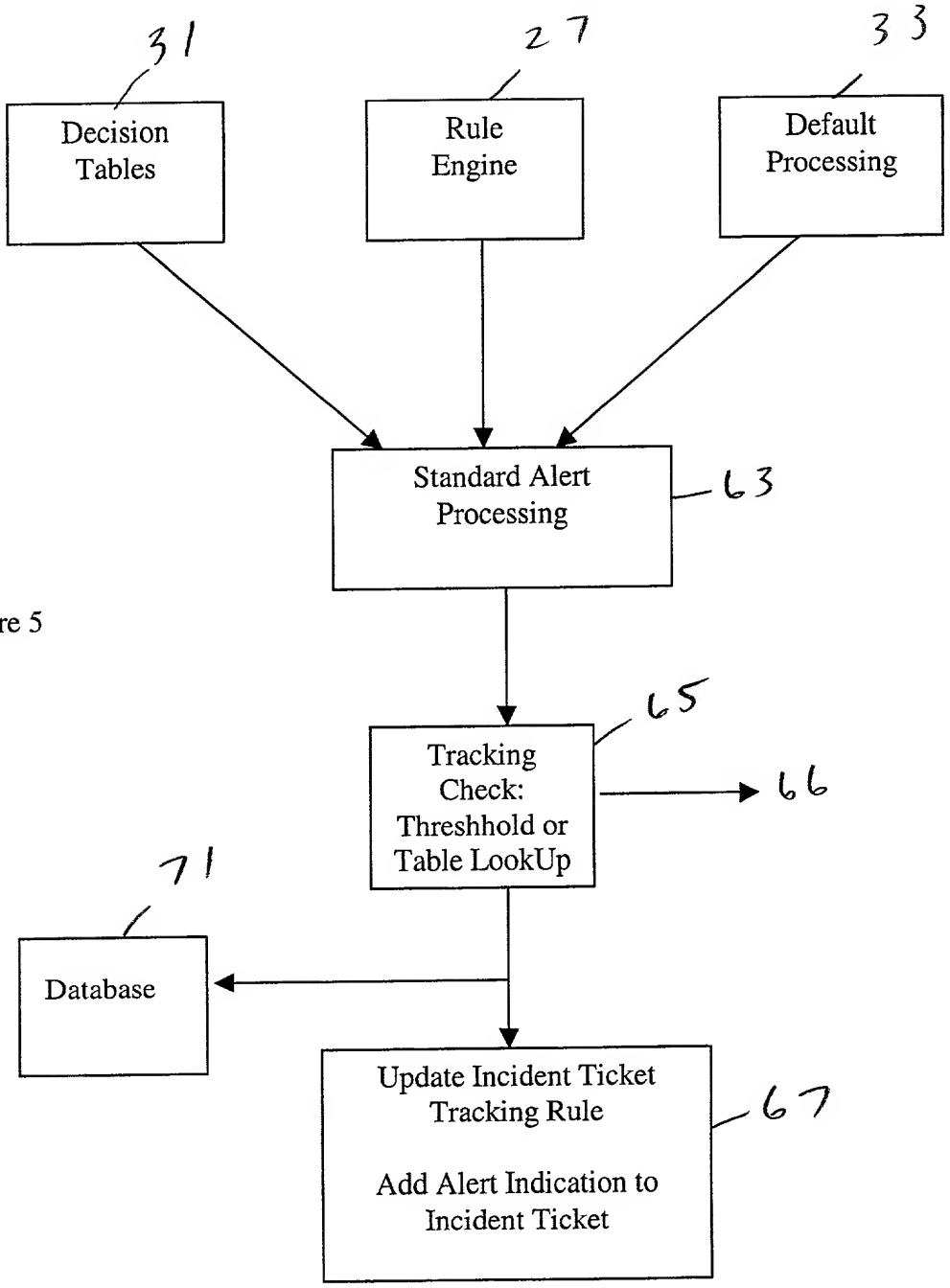


Figure 5

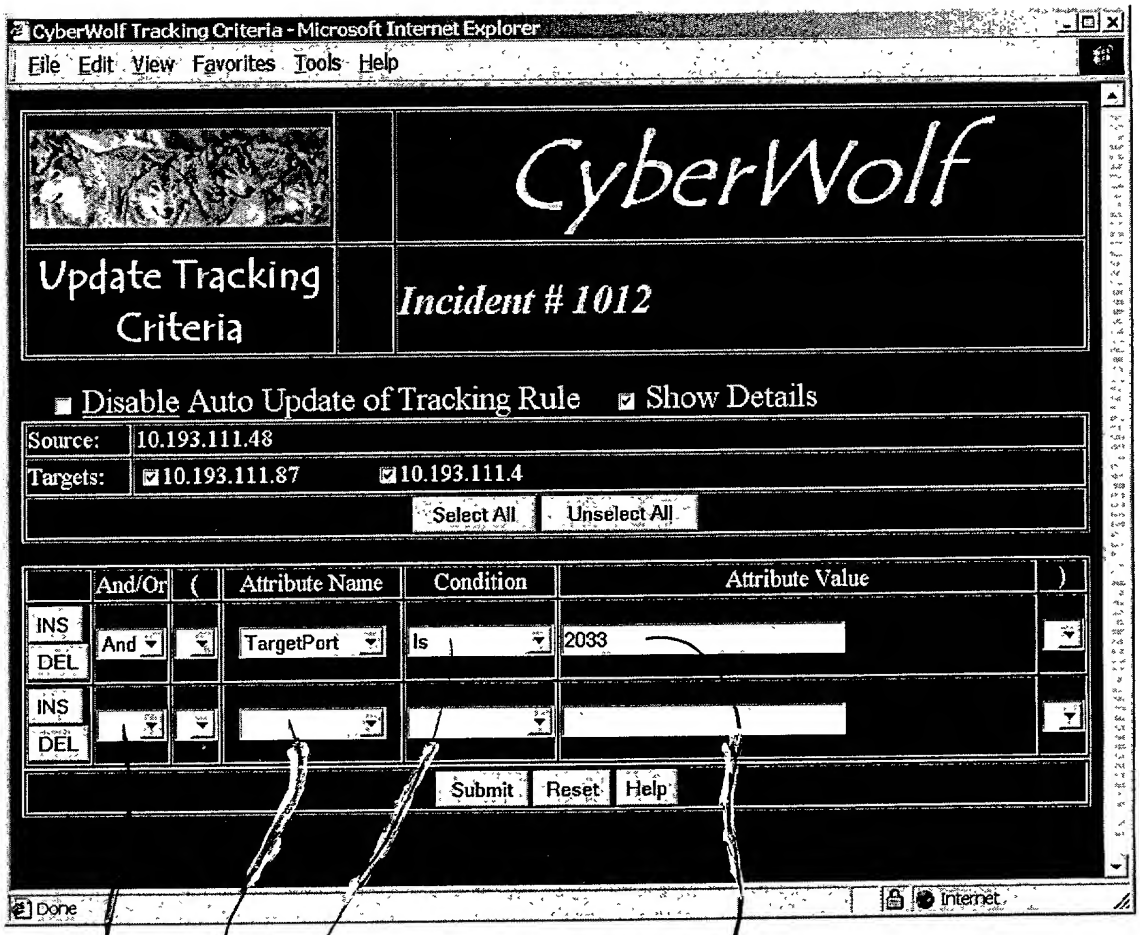

CyberWolf Tracking Criteria - Microsoft Internet Explorer
File Edit View Favorites Tools Help
CyberWolf
Update Tracking Criteria
Incident # 1012
Disable Auto Update of Tracking Rule
Show Details
Source: 10.193.111.48
Targets: 10.193.111.87 10.193.111.4
Select All
Unselect All
And/Or
(
Attribute Name
Condition
Attribute Value
)
INS
DEL
And
TargetPort
Is
2033
Submit
Reset
Help
Done
Internet
77
71
73
75
70

Fig 6